Capítulo 6

Entendendo a Engenharia Social e o No-Tech Hacking

6.1. Objetivos

- Entender o que é Engenharia Social
- Entender o Dumpster Diving
- Entender os riscos associados à Engenharia Social
- Entender as técnicas de No-Tech Hacking

6.2. O que é Engenharia Social?

Podemos considerar a engenharia social como a arte de enganar pessoas para conseguir informações, as quais não deviam ter acesso.

Muitas vezes empregados de uma empresa deixam escapar informações sigilosas através de um contato via telefone ou mesmo conversando em locais públicos como: corredores, elevadores e bares.

Uma empresa pode ter os melhores produtos de segurança que o dinheiro pode proporcionar. Porém, o fator humano é, em geral, o ponto mais fraco da segurança.

“Não existe Patch para a burrice humana”

6.3. Tipos de Engenharia Social

6.3.1. Baseada em pessoas

As técnicas de engenharia social baseada em pessoas possuem diversas características que são utilizadas para que o atacante consiga as informações que deseja, dentre elas podemos citar:

- Disfarces
- Representações
- Uso de cargos de alto nível
- Ataques ao serviço de Helpdesk
- Observações

6.3.2. Baseada em computadores

Esses ataques são caracterizados por utilizarem técnicas de ataque baseadas no desconhecimento do usuário com relação ao uso correto da informática.

Exemplos:

- Cavalos de Tróia anexados a e-mails
- E-mails falsos
- WebSites falsos

6.4. Formas de ataque

6.4.1. Insider Attacks

Insiders são pessoas de dentro da própria organização.

O objetivos por detrás dos ataques de insiders podem ser vários, desde descobrir quanto o colega do lado ganha, até conseguir acesso a informações confidenciais de um projeto novo para vender ao concorrente de seu empregador.

6.4.2. Roubo de identidade

Atualmente, quando alguém cria uma nova identidade baseando-se em informações de outra pessoa, essa identidade é chamada de "laranja".

Dentro de empresas, o roubo de credenciais, para acessar informações que não estão acessíveis a todos, é um fato corriqueiro, que pode passar pelo simples shoulder surfing à clonagem de ID Card.

6.4.3. Phishing Scam

É uma forma de fraude eletrônica, caracterizada por tentativas de adquirir informações sigilosas, ou instalar programas maliciosos na máquina alvo.

Na prática do Phishing surgem artimanhas cada vez mais sofisticadas para "pescar" (do inglês fish) as informações sigilosas dos usuários.

6.4.4. URL Obfuscation

Técnica utilizada para diminuir o tamanho de URL's muito grandes.

Exemplos de serviços:

- migre.me
- okm.me
- digi.to

Isso pode ser utilizado para ocultar URL com parâmetros ou tags maliciosos, como tags de javascript para ataques de XSS, por exemplo.

6.4.5. Dumpster Diving

É o ato de vasculhar lixeiras em busca de informações.

Todos os dias são jogados no lixo de empresas vários documentos por terem perdido sua utilidade. Os atacantes podem aproveitar essas informações e usá-las para um ataque.

6.4.6. Persuasão

Os próprios hackers vêem a engenharia social de um ponto de vista psicológico, enfatizando como criar o ambiente psicológico perfeito para um ataque. Os métodos básicos de persuasão são: personificação, insinuação, conformidade, difusão de responsabilidade e a velha amizade.

Independente do método usado, o objetivo principal é convencer a pessoa que dará a informação, de que o engenheiro social é de fato uma pessoa a quem ela pode confiar as informações prestadas. Outro fator importante é nunca pedir muita informação de uma só vez e sim perguntar aos poucos e para pessoas diferentes, a fim de manter a aparência de uma relação confortável.

6.5. Engenharia Social Reversa

Um método mais avançado de conseguir informações ilícitas é com a engenharia social reversa. Isto ocorre quando o atacante cria uma personalidade que aparece numa posição de autoridade, de modo que todos os usuários lhe pedirão informação. Se pesquisados, planejados e bem executados, os ataques de engenharia social reversa permitem extrair dos funcionários informações muito valiosas; entretanto, isto requer muita preparação e pesquisa.

Os três métodos de ataques de engenharia social reversa são, sabotagem, propaganda e ajuda. Na sabotagem, o hacker causa problemas na rede, então divulga que possui a solução para este, e se propõe a solucioná-lo. Na expectativa de ver a falha corrigida, os funcionários passam para o hacker todas as informações por ele solicitadas. Após atingir o seu objetivo, o hacker elimina a falha e a rede volta funcionar normalmente. Resolvido o problema os funcionários sentem-se satisfeitos e jamais desconfiarão que foram alvos de um hacker.

A melhor referência que atualmente temos sobre engenharia social, é o site do projeto Social Engineering Framework. Para maiores informações acessem:



http://www.social-engineer.org/framework/Social_Engineering_Framework

6.6. No Tech Hacking

Todo e qualquer tipo de ataque que não tenha necessidade de aparatos tecnológicos, nem computadores, são considerados “no tech hackings”.

Esse é método normalmente utilizado para testar a segurança física de uma empresa ou organização, englobando inclusive a engenharia social.

Podemos citar como tipos de ataques “no tech”:

- dumpster diving

- shoulder surfing
- lock picking
- tailgating

6.7. Contramedidas

- Mantenha protegido, não trabalhe em assuntos privados em locais públicos.
- Faça o descarte seguro de documentos.
- Utilize fechaduras e trancas de boa qualidade e comprovado nível de segurança.
- Mantenha bolsas e documentos pessoais em segurança.
- Teste constantemente seus dispositivos de segurança, câmeras e detectores de movimento.
- Tenha cuidado com Shoulder Surfer's.
- Bloqueie o tailgating.
- Mantenha-se atento aos engenheiros sociais.
- Dê treinamento adequado aos funcionários, principalmente os da área de segurança.

6.8. Exercício teórico

Elabore abaixo um script de ataque de engenharia social para conseguir a senha de um usuário.
